CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA

Pametne kartice – siguran nositelj elektroničkog identiteta

Albert Novak – CARNet

CUC 2006, 20.-22.11.2006.

Sadržaj

- Što su to pametne kartice?
- Osnovna svojstva i podjela kartica
- Asimetrična kriptografija
- Infrastruktura javnih ključeva (PKI)
- Pristup resursima putem pametne kartice
- Digitalno potpisivanje korištenjem pametne kartice
- Može li i bez infrastrukture javnih ključeva (PKI)?

Što su to pametne kartice?

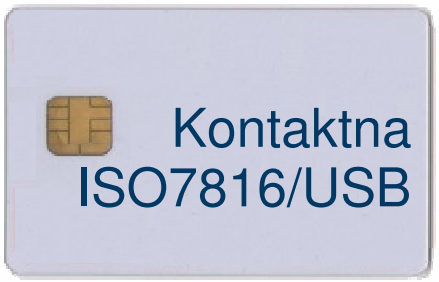
- Plastične kartice standardiziranog formata s ugrađenim µprocesorom, s fizičkim odnosno beskontaktnim sučeljem, eventualno magnetnim stripom, te s reljefnim otiskom i drugim osobinama
- Poseban naglasak na sigurnost podataka i brzinu obrade kritpografskih funkcija
  - kriptografske koprocesore
  - sigurnosne senzore
  - generatore slučajnih brojeva

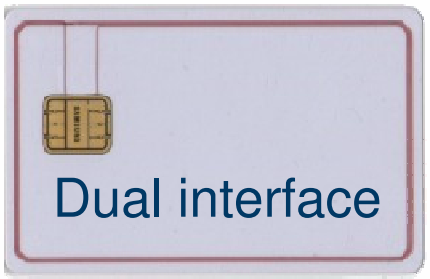
Osnovna svojstva pametnih kartica

- Dvostruka provjera prilikom autentikacije
  - ono što posjeduješ – kartica
  - ono što znaš - PIN
- Sigurna pohrana privatnog ključa
  - privatni ključ nikada ne napušta karticu
- Posjeduju vlastiti operacijski sustav: Java Card, MultOS, OSCCA, Smartcard.NET i sl.
  - omogućavaju pisanje vlastitih aplikacija koje se izvršavaju u sigurnom okruženju
- Specijalno konstruirane za ispunjavanje visokih sigurnosnih standarda

Podjela pametnih kartica

- Sa stanovišta pristupa podacima na kartici/sučeljima:
  - kontaktna, hibridna, dual ili triple interface, beskontaktna
- Sa stanovišta organizacije podataka:
  - datotečna struktura - PKCS15, vlastita struktura podataka – MuscleCard
- Sa stanovišta operacijskog sustava:
  - MultOS, Java Card, Smartcard.NET i sl.



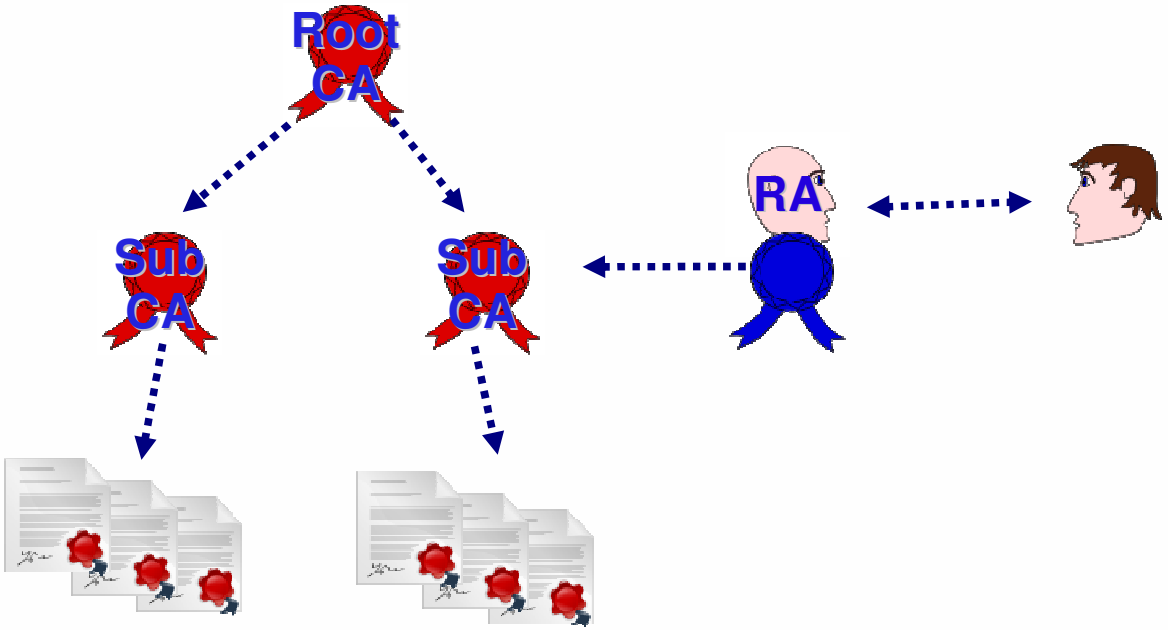


Asimetrična kriptografija

- Bazira se na paru ključeva – privatni i javni ključ
  - poruka kriptirana privatnim ključem može se dekriptirati javnim ključem i obrnuto
- Hash algoritmi omogućavaju nam kreiranje jedinstvenih potpisa – MD5, SHA-1 i sl.
- Certifikati – jednoznačno povezuju niz podataka (certifkat) s privatnim i javnim ključem
- Korištenjem asimetrične kriptografije možemo na siguran način:
  - kriptirati poruke
  - digitalno potpisivati poruke

Infrastruktura javnih ključeva

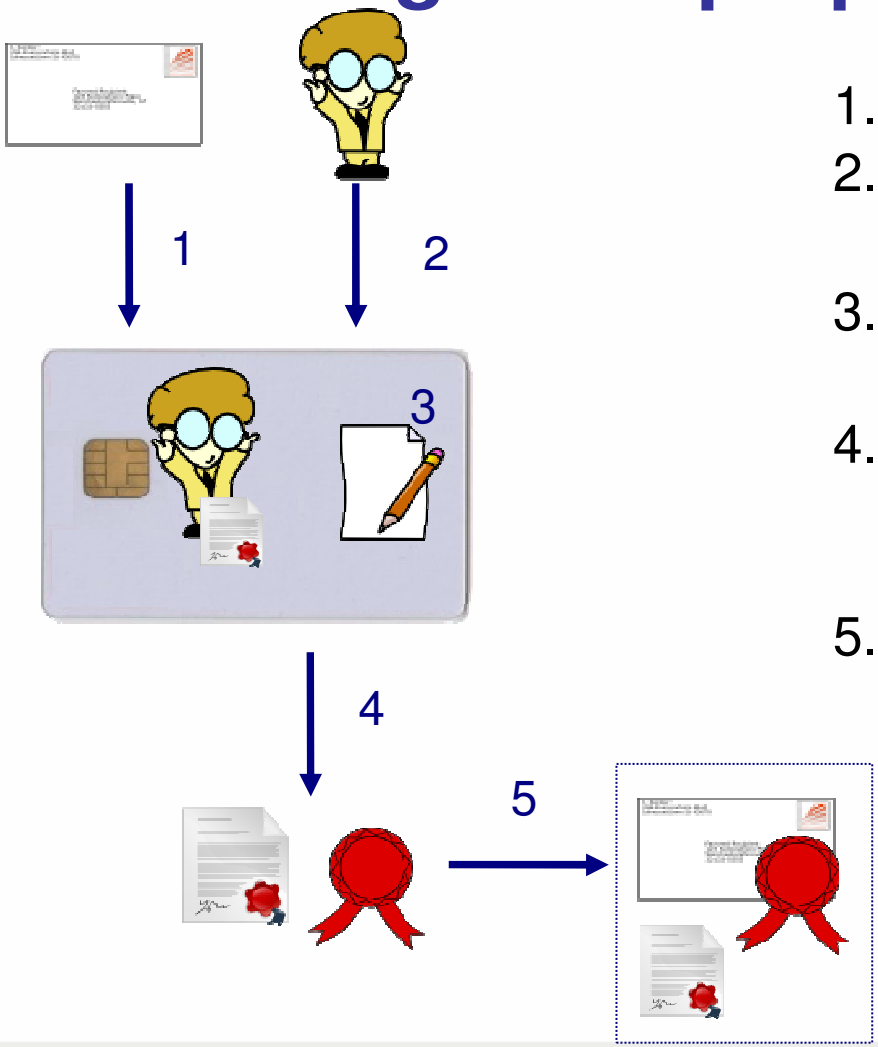
- Da bi elektronički certifikati bili pouzdani potrebno je izraditi infrastrukturu javnih ključeva
  - CA – Certificate Authority
  - RA – Request Authority



Pristup resursima korištenjem pametne kartice

- Prijava na računalo:
  - Windows domenu
  - Linux
- Prijava na Web (apache i IIS)
  - korištenjem SSL-a/TLS-a
- Prijava na mrežu (preklopnik i bežična pristupna točka)
  - korištenjem 802.1x ptorokola
  - radius poslužitelj – EAP-TLS

Digitalno potpisivanje



1. Kreira se hash dokumenta
2. Korisnik PIN-om otključava karticu
3. Na kartici se generira digitalni potpis hash-a dokumenta
4. Aplikacija preuzima digitalni potpis i certifikat s pametne kartice
5. Povezuje se originalni dokument, elektronički certifikat i digitalni potpis. Njihovom provjerom može se ustanoviti vjerodostojnost dokumenta/poruke

Može li i bez infrastrukture javnih ključeva (PKI)?

- GnuPG – postoji podrška za pametne kartice
  - http://www.gnupg.org/(en)/howtos/card-howto/en/smartcard-howto.html
- Udaljeni pristup putem ssh-a – na kartici se čuva par ključeva s kojima se pristupa udaljenom računalu
  - korištenjem opensc podrške u openssh-u
  - korištenjem pkcs11 modula
- CACert – besplatni certifikati
  - http://www.cacert.org/
- PKI infrastruktura može se jednostavno izgraditi korištenjem već dostupnih alata:
  - MicrosoftCA
  - OpenCA ili OpenXPKI

I na kraju ...

- Pametne kartice omogućavaju nam sigurno čuvanje podataka:
  - privatni ključ u asimetričnoj kriptografiji
  - osobni podaci
  - e-novčanik
- U zavisnosti od sigurnosnih postavki appleta na kartici omogućavaju jednostavan SSO i to ne samo za web resurse
  - kartice može imati takve sigurnosne postavke da je dovoljno samo jedanput unijeti PIN za pristup privatnom ključu povezanom s certifikatom
- Zahtjeva dodatna ulaganja pa treba ocijeniti gdje je stvarno opravdano uvođenje sigurnosnih mehanizama koje nam omogućava pametna kartica

... i još par linkova

- Muscle - http://www.linuxnet.com/
- OpenSC - http://www.opensc-project.org/
- CoolKey - http://directory.fedora.redhat.com/wiki/CoolKey
- OpenCA - http://www.openca.org
- OpenXPKI - http://www.openxpki.org
- PKI Lab - http://www.dartmouth.edu/~deploypki/
- CAcert - http://www.cacert.org/
- GnuPG - http://www.gnupg.org/(en)/howtos/card-howto/en/smartcard-howto.html